

101年公務人員特種考試警察人員考試、
101年公務人員特種考試一般警察人員考試及
101年特種考試交通事業鐵路人員考試試題

代號：20160

全一頁

等 別：二等一般警察人員考試

類 科：刑事警察人員數位鑑識組

科 目：網路與資訊安全（包括資訊安全技術與應用、資安事件處理）

考試時間：2 小時

座號：_____

※注意：(一)禁止使用電子計算器。

(二)不必抄題，作答時請將試題題號及答案依照順序寫在試卷上，於本試題上作答者，不予計分。

一、名詞解釋：

(一) X.509 (5 分)

(二)時序攻擊法 (Timing Attack) (5 分)

(三)蠕蟲 (Worm) (5 分)

(四)隔離區 (Demilitarized Zone, DMZ) (5 分)

二、根據統計，企業中資訊安全事故有 80%是來自內部員工，因為資安事故無法完全由技術面來解決，因此在管理面要有相對之資訊安全政策。請問：

(一)什麼是政策 (Policy)？什麼是運作程序 (Procedure)？兩者之不同處為何？
(10 分)

(二)請列舉 3 項資訊安全政策應考慮之重點，並詳細說明之。(10 分)

三、入侵偵測系統 (Intrusion Detection System, IDS)：

(一)什麼是主機型入侵偵測系統 (Host-based Intrusion Detection System)？什麼是網路型入侵偵測系統 (Network-based Intrusion Detection System)？兩者有何不同？
(10 分)

(二)什麼是誘捕系統 (Honeypots)？裝置誘捕系統之 2 個主要目的為何？(10 分)

四、交談金鑰 (Session Key)：

(一)什麼是交談金鑰？交談金鑰之特性為何？(10 分)

(二)交談金鑰的產生有 2 個主要方法。一種是利用主金鑰 (Master key)；另一種是利用金鑰交換 (Key Exchange) (如：Diffie-Hellman 金鑰交換)，請分別說明此 2 種方法之運作方式。(10 分)

五、串流加密 (Stream Cipher)：

(一)請問什麼是串流加密？串流加密通常在什麼情況下使用？(10 分)

(二)串流加密產生器 (Stream Cipher Generator) 在設計上有 2 個需求，請詳述之。
(10 分)